

of toll fraud for periods longer than a day. As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

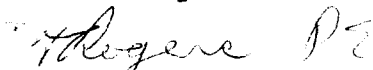
The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

Kansas Turnpike Authority


Thomas A. Rogers, P.E.
Communications Engineer

TAR/jmt



H.B. Zachry Company

ORIGINAL

January 10, 1993

RECEIVED

JAN 14 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd _____
List A B C D E

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script, reading "Helen Bryan". The signature is written in dark ink and is positioned below the "Sincerely," text.

ORIGINAL

January 11, 1993

RECEIVED

JAN 14 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by IXC's, LEC's and CPE's the law should reflect that. It is preposterous to think that the IXC's, LEC's and CPE's who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop toll fraud.

CPE's should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPE's ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPE's should be required to include security related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

SPECIALIZED
BICYCLE COMPONENTS
15130 CONCORD CIRCLE
MORGAN HILL
CALIFORNIA 95037
408-779-6229

No. of Copies rec'd
List A B C D E

Orig.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, LECs should be required to offer monitoring services similar to IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

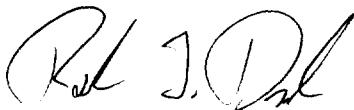
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and give law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to read 'R. J. Dzek', with a stylized flourish at the end.

Raymond J. Dzek
Operations Supervisor
Specialized Bicycle Components
15130 Concord Circle
Morgan Hill, CA 95037

ORIGINAL



P.O. BOX 511
EL PASO, TX 79961-0001
PHONE: 915-594-5500
FAX: 915-594-5699

January 10, 1994

Mr. William F. Canton, Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

RECEIVED

JAN 14 1994

FCC MAIL ROOM

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communication systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue have absolutely no legal obligations to warn customers and therefore no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design of the car - not an adjunct that you have to purchase later.

No. of Copies rec'd

1154 HAWKINS BLVD. • EL PASO, TEXAS 79945

1st A B C D E

Orig

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies such as El Paso Water Utilities and the educational information supplied is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any case of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LEC's should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause. The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to read 'John E. Balliew', with a long horizontal flourish extending to the right.

John E. Balliew, P.E.
Environmental Compliance Manager



41-60 MAIN STREET • FLUSHING, N.Y. 11355-3820

January 10, 1993

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

0

RECEIVED
JAN 14 1994
FCC MAIL ROOM

SYSTEMS & PROCEDURES
Telephone (718) 670-7596

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script, reading "Colleen M. Fay". The signature is written in dark ink on a white background.

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RECEIVED

JAN 14 1994

FCC MAIL ROOM

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

1 copy

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Connie North
Telecommunications Mgr
GE-CBS

BESSEMER AND LAKE ERIE RAILROAD COMPANY

135 JAMISON LANE • P. O. BOX 68 • MONROEVILLE, PENNSYLVANIA 15146

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

RECEIVED

JAN 14 1994

FCC MAIL ROOM

RE: CC DOCKET 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communication systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car, not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

No. of Copies rec'd
List ABCDE

0

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

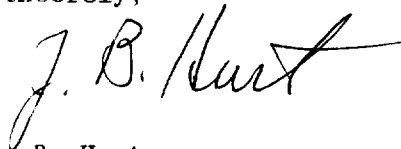
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

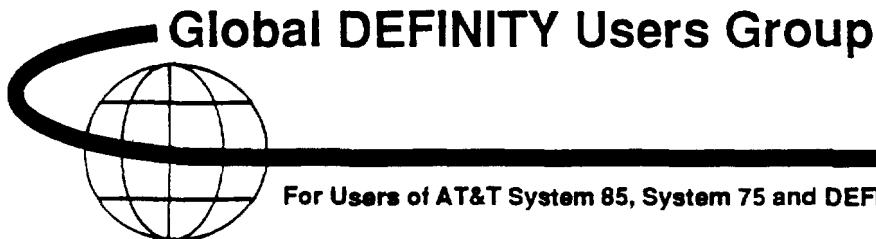
Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to read "J. B. Hurt". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

J. B. Hurt
Telecommunications Specialist



Global DEFINITY Users Group

For Users of AT&T System 85, System 75 and DEFINITY® PBXs

January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket No. 93-292

Reneé Seay
President
Advanced Micro Devices
901 Thompson Place MS10
Sunnyvale, CA 94088
408-749-3269
FAX 408-749-5299

JAN 14 1994

FCC MAIL ROOM

Dear Mr. Canton:

As President of the Global DEFINITY Users Group I represent 800 AT&T PBX users. Most of these users have multiple PBX installations, and although they have taken steps recommended by the Users' Group and AT&T to reduce the risk of telecommunications fraud, they are still vulnerable. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Spring Guard, MCI Detect, and AT&T Netprotect) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud that precipitate for lengths greater than 24 hours.

LEC's must also provide monitoring and proper notification as part of their basic service offerings. Local lines are just as vulnerable to toll fraud. The definitive line between IXC and LEC is becoming fuzzier, and therefore monitoring and proper notification by all carriers is of vital importance to the fight against telecommunications fraud.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE

No. of Copies rec'd 023
List A B C D E

vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment, and to provide solutions to assist customer's in reducing the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed to the customer at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format, CPE vendors should also be encouraged to offer security related hardware and software in their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

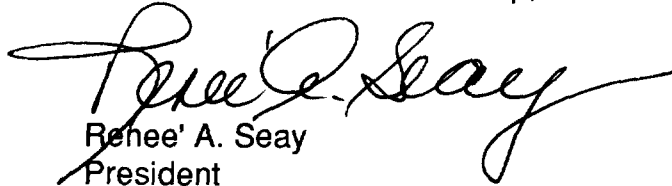
- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- ISCs and LECs to offer detection, notifications, prevention, and educational based offerings and services

If toll fraud occurs due to the negligence of one or more parties, then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitably distributed among the CPE owner, all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we will make a positive impact on this problem.

Sincerely,

Global DEFINITY Users Group, Inc.



Renee A. Seay
President



January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RE: CC Docket 93-292

JAN 14 1994

FCC MAIL ROOM

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXCs and CPE vendors to secure my systems, toll fraud is still possible. It is impossible to secure my systems 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we do not control 100% of our destiny. Since our destiny is not only controlled by our systems' security precautions, but also by the information, services and equipment provided by the IXCs, LECs, and CPE vendors, the law should reflect that. It is preposterous to think that the IXCs, LECs, and CPE vendors who all have a very important part in this issue, have absolutely no legal obligations whatsoever. to warn customers, and therefore no real incentive to stop fraud.

CPE vendors should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPE vendors ship equipment without default passwords which are well known within the hacker community. Passwords should be created during installation of the equipment with the customer's full knowledge. CPE vendors should be required to include security-related hardware and software in the price of their systems.

While the programs offered by the IXCs, such as MCI Detect, AT&T NetProtect, and SprintGuard have broken new ground in relation to preventing toll fraud, they still do not do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there should not be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd 024
List A B C D E

Page 2
RE: CC Docket 93-292
January 12, 1994


As hackers find new methods of breaking into our systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and education. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the toll fraud problem and not the cause. The root of this insidious crime is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communications systems. Hackers continue to try and convince us that they only hack to gain knowledge. While they are the ones that actually break into our systems and sell the information, it is the 'call sell' operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Sincerely,



Peter J. Guile
Manager, Network Services

cc: Mr. Spencer F. Barber
Mr. Michael W. Mann



JAN 14 1994

FCC MAIL

SDN Users Association, Inc.

P.O. Box 4014, Bridgewater, NJ. 08807

January 13, 1994

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 M Street NW
Washington, DC 20554

RE: FCC Docket Number 93-292
"Policies & Rules Regarding Toll Fraud"

Dear Mr. Caton:

The SDN Users Association, Inc. represents more than 370 large users of domestic and international telecommunication services from all sectors of the economy. Unfortunately, many of our member companies have had first hand experience with toll fraud. The Association commends the Federal Communications Commission for its vision in proposing rules to clarify responsibilities in toll fraud cases.

We believe that the network providers, PBX/Equipment manufacturers as well as the customers must share in the responsibility for eliminating toll fraud and ultimately share in the financial liability. The Association has partnered with AT&T to virtually eliminate Network Remote Access toll fraud. However, we still see the sophistication of those penetrating toll fraud rising faster than the level of protection afforded by network providers and equipment manufacturers in other areas.

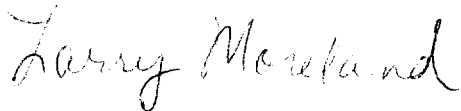
Although AT&T NetPROTECT, MCI Detect and SprintGuard offer carrier fraud protection programs, they still have limitations, associated costs, and restrictions. In effect they are insurance policies that the user must subscribe to and pay for and still only receive limited protection.

No. of Copies rec'd 2
List A B C D E

The SDN Users Association, Inc. would like to propose the development of standards for all parties providing telecommunication equipment and services. The Association also sees the need for additional federal laws that would strengthen and enforce prosecuting telephone related fraud.

The SDN Users Association, Inc. would like to offer our first hand knowledge to help evaluate and develop standards regarding docket #93-292. We see evolving technology that will present future challenges and will require ongoing policy and standards review.

Sincerely yours,

A handwritten signature in cursive script that reads "Larry Moreland".

Larry Moreland, President
SDN Users Association, Inc.



HIMONT U.S.A., Inc.
Three Little Falls Centre
2801 Centerville Rd.
P.O. Box 15439
Wilmington, DE 19850-5439

Tel. 302-996-6000
Fax 302-996-6051

January 13, 1994

Office of the Secretary
Federal Communications Commission
Washington DC 20554

JAN 14 1994

FCC MAIL ROOM

RE: REFERENCE NUMBER CC Docket 93-292

Himont USA Inc., has been a victim of and is concerned with toll fraud. Himont would like to comment on the NPRM that is the subject of the above mentioned docket.

Himont feels that the carriers and equipment vendors should be required to provide customers with methods, programs, and/or equipment that will prevent toll fraud on their service or equipment. The carriers and equipment providers should have to make the availability of these fraud prevention methods, programs, and/or equipment known to the customer as part of the monthly billing statement for said service or equipment. Himont feels that the carriers and equipment vendors are in the best position to warn customers about exposure to toll fraud, due to their experience with a variety of accounts, expertise in their field, and access to engineering, programming & proprietary information about the service & equipment that they manufacture, service, maintain or provide.

The equipment vendors and carriers should be required to prominently label equipment, training manuals, software packages, and hardware and software upgrades, with labels warning that customers are subject to toll fraud based on the product's use. In addition, documentation must be provided that clearly outlines how the product can be effectively used in a manner that enables fraud to be prevented. This information must be disclosed prior to the sale of any new equipment or services. Detail information warning of potential exposure and methods to avoid fraud on existing equipment and services, should be provided to the customer on a regular basis.

Audits of the customer's equipment and services for fraud vulnerability should be made available to the customer from the vendor or carrier providing the equipment or service. These audits need to warn customers that they are subject to toll fraud and how the potential fraud can be prevented.

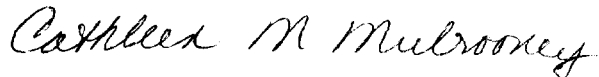
No. of Copies rec'd 014
LIST A B C D E

The FCC needs to clearly outline the various categories of telecommunications equipment and services, for example: Customer Premise Equipment, cellular equipment and the various carriers services. Within these categories, the FCC needs to detail what liability the vendor and customer have related to toll fraud.

Himont feels that the equipment vendors and carriers have a responsibility to provide services and information to help in detection and prevention of toll fraud. Lack of equipment vendor and carrier responsibility in this area leaves the situation for toll fraud open to escalate in its severity, as there is little, if any, incentive to these entities to aid such victims as CPE customers in avoiding such fraud, which presently seems to impact only the pocket of the customer. Further, we find it confusing and unfair that Customer Premise Equipment fraud is solely the liability of the customer, when the victim of calling card fraud and payphone booth fraud has limited liability.

Further, Himont feels that the perpetrators of these crimes must be punished in a manner that will deter continued toll fraud. Presently efforts and regulations to punish these criminals seem ineffective.

Respectfully submitted,



Cathleen M. Mulrooney
Senior Telecommunications Specialist

cc: Deanna Kelly	Himont USA, Inc. Legal Counsel
Bill Noonan	Himont USA, Inc. GM Business Process Technology Director & Worldwide Director of Information Services



Global DEFINITY User's Group

For User's of AT&T System 85, System 75 abd DEFINITY PBXs

101 Skeet Circle East
Bear, DE 19701
January 12, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

JAN 14 1994
FCC MAIL ROOM

Re: CC Docket no. 93-292

Dear Mr. Canton:

As Chairman of the Security Committee in the Global Definity User's group I represent 800 AT&T PBX users. Most of these users have multiple PBX installations, and although they have taken steps recommend by the User's Group and AT&T to reduce the risk of telecommunications fraud, they are still vulnerable. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud that precipitate for lengths greater than 24 hours.

No. of Copies rec'd
List A B C D E

043

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are just as vulnerable to toll fraud. The definitive line between IXC and LEC is becoming fuzzier, and therefore monitoring and proper notification by all carriers is of vital importance to the fight against telecommunications fraud.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment, and to provide solutions to assist customer's in reducing the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed to the customer at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should also be encouraged to offer security related hardware and software in their systems.

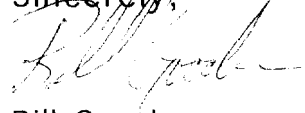
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and educational based offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among the CPE owner, all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we will make a positive impact on this problem.

Sincerely,

A handwritten signature in dark ink, appearing to read "Bill Gooden", written over the word "Sincerely,".

Bill Gooden
Chairman
Security Committee
Global Definity Users Group